What is claimed is:

1. A system for providing instant, automatic, and secure log-in to a network server for a portable device (PD) logging in to the network server via a first computer station acting as an Internet Host (IH) for the PD, the system comprising:

first software executing on the computer station, including a location token (H-token) generator and a storage location reserved for the H-token;

second software executing on the network server, including a password code (P-token) generator, and one or more tables relating P-tokens, H-tokens, and subscriber's user names and passwords; and

third software executing on the PD, and a storage location on the PD reserved for the P-token;

characterized in that, upon a log-in request signal to the IH from the PD, the IH opens a communication link to the network server, requests the P-token from the PD, and, receiving the P-token, furnishes both the P-token and the IH-stored H-token, if any, to the network server, and the network server, only upon finding a match between P-token, H-token, and a valid subscriber, validates log-in without requesting user name and password.

2. The system of claim 1 wherein the first time a subscriber requests log-in from a PD having no valid stored P-token, the network server requests the subscriber's user name and password, then creates a P-token, which is transmitted to the IH, and from the IH to the PD, where the PD stores the P-token for future log-in operations.

3. The system of claim 1 wherein the first time a subscriber requests log-in from a PD having a valid P-token through an IH having no valid stored H-token, the IH generates a new H-token, stores the new H-token in the storage location reserved for it, then furnishes the P-token and the new H-token to the network server, which requests user name and password for log in, and receiving a valid user name and password, grants log-in, and stores the new H-token associated with the user and the P-token for future log-in operations, thus validating a new IH location for valid instant log-in.

4. The system of claim 1 wherein, in the absence of either a valid P-token or a valid H-token, the network server requests user name and password for log-in, and refuses log-in if the user name and password are not for a valid subscriber.

5. The system of claim 1 wherein the network server is a Web server connected to the Internet.

6. A method for providing instant, automatic, and secure log-in to a network server for a portable device (PD) logging in to the network server via a first computer station acting as an Internet Host (IH) for the PD, the method comprising steps of:

(a) upon receiving a log-in request signal by the IH from the PD, opening by the IH a communication link to the network server, requesting by the IH a password code (P-token) from the PD, and, receiving the P-token, furnishing both the P-token and an IH-stored location code (H-token) to the network server; and

(b) upon finding a match by the network server between P-token, H-token, and a valid subscriber, validating log-in without requesting user name and password.

7. The method of claim 6 further comprising a step for, the first time a subscriber requests log-in from a PD having no valid stored P-token, requesting by the network server the subscriber's user name and password, then creating a P-token, transmitting the new P-token to the IH, and from the IH to the PD, and the PD storing the new P-token for future log in operations.

8. The method of claim 6 further comprising a step for, the first time a subscriber requests log-in from a PD having a valid P-token through an IH having no valid stored H-token, the IH generating a new H-token, storing the new H-token in the storage location reserved for it, then furnishing the P-token and the new H-token to the network server, which requests user name and password for log in, and receiving a valid user name and password, granting log-in, and storing the new H-token associated with the user and the P-token for future log-in operations, thus validating a new IH location for valid instant log-in.

9. The method of claim 6 wherein, in the absence of either a valid P-token or a valid H-token, the network server requests user name and password for log-in, and refuses log-in if the user name and password are not for a valid subscriber.

10. The method of claim 6 wherein the network server is a Web server connected to the Internet.